UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,512	01/20/2004	Philippe Leyendecker	PF030028	2983

7590 08/16/2010

JOSEPH S. TRIPOLI
THOMSON LICENSING INC.
SUITE 200
2 INDEPENDENCE WAY
PRINCETON, NJ 08540

EXAMINER	
PARRA, OMAR S	

ART UNIT	PAPER NUMBER
2421	

MAIL DATE	DELIVERY MODE
08/16/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/761,512	LEYENDECKER ET AL.	
	Examiner	Art Unit	
	OMAR PARRA	2421	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-13,15-19,21-24,26 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-13,15-19,21-24,26 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, see Remarks section page 12, filed 04/29/2010, with respect to the rejection(s) of claim(s) 1 and 13 under U.S.C 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Benardeau, Peterka and Wehrenberg.

Although the examiner is presenting new grounds of rejection, the examiner believes necessary to address some of applicant's arguments.

Applicant argues: *Benardeau teaches a master-slave couple that is paired and which requires the slave to request information from the master, whereas Peterka teaches a system in which either each client request new keys or a server sends the keys to the clients....Why would the skilled person combine the paired solution Benardeau with the non-paired solution of Peterka when it would seem so much easier to entirely one mode and simply use Peterka without Benardeau. The answer would appear to be impermissibly hindsight construction with the present claims in mind, in contravention of, for example, MPEP §2141.01(III)".* Remarks, page 9. To this matter, the examiner respectfully disagrees.

Benardeau teaches a master-slave couple of devices that can update their security keys (at least, abstract). Benardeau besides the communication between the two devices, can also permit direct communication between the content distribution and the slave, where the content distribution can directly send messages to the slave device (col. 14 lines 51-59).

Peterka teaches a system that in which the server can contact the slave device, as noted by the applicant. Peterka teaches a system that distributes ECM and EMM messages in order to update encryption keys (title, [0106]); [0123]). Peterka teaches different models of content distribution; among them a subscription model ([0003]; [0098]), in which the user pays a monthly fee for receiving content. In this model, the server provides, at the beginning a key with which the user can consume the content for the first time and after that, the key is updated and it's valid for a period of time ([0098], [0099]). When distributing the keys, Peterka teaches that the system could use the 'Push' model, in which the server keeps track of the expiration date of the keys and sends messages with the new key to delete the old ones ([0106]-[0109]).

Therefore, being both systems for updating security keys and being both systems able to send messages to the devices connected to the server, a person skilled in the art would have found no problem to combine both references.

2. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was

within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

"Peterka is completely silent regarding the feature of instructing the clients to delete the information", Remarks page 10. To this matter, the examiner respectfully disagrees.

In either one of the methods, the server sends EMM or ECM messages (table 1, page 7; [0106]) for the clients to replace a first key with a second key before the first key expires ([0107]-[0110]; [0113]-[0014]). Therefore, with the reception of the second message, the client is informed to replace the expired first key.

Claims 19, 22 and 27:

Applicant argues that *"there is simply no mention or hint at a combination that lets the slave receive filter parameters from the master, and that those parameters enable extraction of the access entitlements by the slave",* page 15. To this matter, the examiner respectfully disagrees.

Benardeau teaches sending CW from the master to the slave device (col. 13 lines 11-38; col. 11 line 54- col. 12 line 8; col. 14 line 48- col. 15 line 32), in addition to additional data with entitlements for the slave. The messages from the master are encrypted with the key Ks, leaving everything else not encrypted with this key Ks

(encrypted content received by the distribution center) filtered out in the master-slave communication.

On the other hand, Peterka teaches that the terminal has filters to separate between information. Peterka teaches a system that distributes ECM and EMM messages in order to update encryption keys (title, [0106]); [0123]). Peterka teaches different models of content distribution; among them a subscription model ([0003]; [0098]), in which the user pays a monthly fee for receiving content. In this model, the server provides, at the beginning a key with which the user can consume the content for the first time and after that, the key is updated and it's valid for a period of time ([0098], [0099]). When distributing the keys, Peterka teaches that the system could use the 'Push' model, in which the server keeps track of the expiration date of the keys and sends messages with the new key to delete the old ones ([0106]-[0109])

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims **1-7, 9-13, 15-18, 21 and 25** are rejected under 35 U.S.C. 103(a) as being unpatentable over Benardeau et al. (hereinafter 'Benardeau', Patent No. 6,904,522,

which is of record) in view of Peterka et al. (hereinafter 'Peterka', Pub. No. 2002/0170053) in further view of Wehrenberg (Pub. No. 2003/0126445).

Regarding claims 1 and 13, Benardeau teaches a system for receiving broadcast digital data comprising:

a master digital terminal **(12, Fig. 4; col. 12 lines 46-55)** and at least one slave digital terminal **(50, Fig. 4; col. 12 lines 56-62)** adapted to generally simultaneously receive protected digital data from a transmitter **(col. 8 lines 1-10; col. 12 lines 56-62; col. 13 lines 29-33; col. 14 lines 51-59)**, the at least one slave digital terminal being connected to the master terminal by a link **(51, Fig. 4)**,

Although Benardeau teaches that the master terminal provides the slave terminal with the information necessary for accessing said protected digital data within a predetermined deadline (col. 13 lines 11-38; col. 11 line 54- col. 12 line 8; col. 14 line 48- col. 15 line 32; where the predetermined deadline is the validity period or life of the Kex and/or CW. The master device has to send the CW to the slave before its validity changes. Or, when the CW is sent to the slave, it's encrypted with a Ks- a session key- that's generated by the slave. This key also has a predetermined time, col. 14 lines 16-24. Without the Ks, no encryption would be possible to transmit CW and no reception of the information necessary for accessing the content would be safely received, which goes against the principle of having a safe link), Benardeau does not explicitly teach having the slave digital terminal to receive a message from a transmitter instructing to said at least one slave digital terminal to delete stored information necessary for

accessing said protected digital data, to request, after receiving the message, new information necessary for accessing said protected digital data from its repository, and that the slave awaits a predetermined deadline counted from a transmission of the request.

However, in an analogous art, Peterka teaches a system that distributes ECM and EMM messages in order to update encryption keys (title, [0106]); [0123]). Peterka teaches different models of content distribution; among them a subscription model ([0003]; [0098]), in which the user pays a monthly fee for receiving content. In this model, the server provides, at the beginning a key with which the user can consume the content for the first time and after that, the key is updated and it's valid for a period of time ([0098], [0099]). When distributing the keys, Peterka teaches that the system could use the 'Push' model, in which the server keeps track of the expiration date of the keys and sends messages with the new key to delete the old ones ([0106]-[0109]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified Bernardeau's invention with the reception of a delete message as taught by Peterka for the benefit of reminding the terminals that expiration time of the key is close and needs to be updated for not having the service interrupted.

Additionally, Benardeau and Peterka do not explicitly teach that the requesting device awaits a predetermined deadline counted from a transmission of the request.

However, in analogous art, Wehrenberg teaches a device that when it requests a key from a device that possesses it, it only awaits for a predetermined amount of time

for the key and if it does not receive it during this time, the device stops its video decoding and recording activity ([0085]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified Benardeau and Peterka's invention with Wehrenberg's feature of implementing a timeout period when the receiving device requests keys from the source device and terminate communication if the response takes longer than a time tolerance for the benefit of avoiding communication with a tampered device.

Regarding claim 2, Benardeau, Peterka and Wehrenberg teach a system, wherein the information necessary for accessing the protected data which is received by the master digital terminal originates from a data broadcasting system **(Benardeau: 41, Fig. 3; col. 11 lines 54-65).**

Regarding claim 3, Benardeau, Peterka and Wehrenberg teach a system wherein said information for accessing the data received by the master digital terminal is transformed before being sent to the slave digital terminal **(Benardeau: col. 3 lines 24-29, lines 52-61; col. 14 line 60-col. 15 line 32)**.

Regarding claims 4 and 6, Benardeau, Peterka and Wehrenberg teach a system, in which the transformation comprises a descrambling of said information in the master digital terminal, the descrambling being performed with the aid of keys received

beforehand by the master digital terminal of the broadcasting system **(Benardeau: Kex, used to descramble CW is received in advance by terminal 12, col. 13 lines 11-38; col. 14 line 60- col. 15 line 32)**.

Regarding claim 5, Benardeau, Peterka and Wehrenberg teach a system, wherein the information necessary for accessing the protected data, which is received by the master digital terminal, originates from the slave digital terminal, is transformed before being resent to the slave digital terminal **(Benardeau: CW can be sent to the master device or originated from the slave for further descrambling at the master and being sent back to the slave, col. 14 line 51- col. 15 line 32)**.

Regarding claim 7, Benardeau, Peterka and Wehrenberg teach a system, in which the protected digital data comprise television services scrambled by keys and in which the information necessary for accessing said data belongs to the set comprising:

- a message containing access entitlements to the services for the slave digital terminal **(Benardeau: ECM is sent to slave, and checked by master for slave's rights, col. 9 lines 25-51; col. 14 lines 51-65)**;

-a message containing parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal **(Benardeau: EMM monthly update of Kex, lets decipher the ECM that contains rights of slave and Control Word, col. 11 line 66- col. 12 line 8).**

- a message **(62, Fig.5)** containing partial information **("KpubT" or 68, Fig. 5, partial information -one of the pair of keys needed to have communication after authentication)** enabling the slave digital terminal to reconstruct its access entitlement to the services **(Benardeau: Without the KpubT, no communication is possible and therefore the reconstruction of access entitlement –ECM- is consequently no possible)**;

- a message containing keys for descrambling said protected digital data **(Benardeau: ECM containing Control Word, and EMM containing Kex update, which are used to descramble the protected content, col. 7 lines 3-9)**.

Regarding claim 9, Benardeau, Peterka and Wehrenberg teach a system in which the predetermined deadline is counted down from the dispatching by the broadcasting system of the data of a message to the master digital terminal **(Benardeau: It's the broadcasting system which dispatches the Kex for giving rights for a predetermined period of time; therefore, for renewing it, the broadcasting system has to keep track or count down the remaining time of the Kex)**.

Regarding claims 10, Benardeau, Peterka and Wehrenberg teach a system, in which the information necessary for accessing the protected data is sent from the master digital terminal to the slave digital terminal while being protected by enciphering using key shared by the two terminals **(Benardeau: col. 15 lines 4-32)**.

Regarding claim 11, Benardeau, Peterka and Wehrenberg teach a system in which

the master digital terminal and slave digital terminal furthermore receive from the data broadcasting system a secret code **(Benardeau: Sprit and KpubT pair of keys, which are respectively received by master and slave, 64 and 68, Fig. 5)** and,

in which the master digital terminal sends said information necessary for accessing the data to the slave terminal only if it receives said secret code from the slave terminal within a second predetermined deadline counting down the receipt of the secret code by the master terminal **(Benardeau: When the CW is sent to the slave, it's encrypted with a Ks- a session key- that's generated by the slave. This key also has a predetermined time, col. 14 lines 16-24. Without the Ks, no encryption would be possible to transmit CW and no reception of the information necessary for accessing the content would be safely received, which goes against the principle of having a safe link).**

Regarding claim 12, Benardeau, Peterka and Wehrenberg teach a system in which the secret code received by the master digital terminal and by the slave digital terminal is scrambled with the aid of keys sent beforehand to said terminals by the data broadcasting system **(Benardeau: KpubT is encrypted with Ceriman, which is the pair of Clubman received by the slave receiver. The certificate that contains the encrypted KpubT and more, is encrypted using the exploitation key Kex, which is sent to the master device in advance; col. 13 line 53-col. 14 line 15)**.

Regarding claims 15 and 16, Benardeau, Peterka and Wehrenberg teach a system wherein the information necessary for accessing said protected data comprises a secret key **(Benardeau: Control Word used to descramble the content is a key, col. 7 lines 3-9; col. 14 line 51- col. 15 line 32)**.

Regarding claims 17 and 18, Benardeau, Peterka and Wehrenberg teach a system wherein the protected digital data is received via another link **(Benardeau: col. 12 lines 56-62)**.

Regarding claim 21, Benardeau, Peterka and Wehrenberg teach a system, wherein the slave decoder is adapted to block by longer accepting the information necessary for accessing said protected digital data from the master decoder **(Benardeau: The decoder that is adapted to block, not being able to display content, can be blocked by longer even if the information necessary for accessing said protected digital data –CW- from the master is accepted. This happens when the Ks is not generated when the content is a pay per view film that has not been paid, col. 14 lines 16-24).**

Regarding claim 25, Benardeau, Peterka and Wehrenberg teach wherein the at least one slave digital terminal actively blocks by cancelling stored information necessary for access **(Benardeau: As one of ordinary skill in the art will**

immediately notice, when the new keys do not arrive to the slave before their validity time, the old or stored keys are not valid anymore and the presentation is blocked).

5. Claims **19, 22, 26 and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over Benardeau et al. (hereinafter 'Benardeau', Patent No. 6,904,522, which is of record) in view of Akiyama (Pub. No. 2006/0212399).

Regarding claims 19, 22, 26 and 27, Benardeau teaches a system for receiving broadcast digital data, comprising:

a master digital terminal **(12, Fig. 4; col. 12 lines 46-55)** and at least one slave digital terminal **(50, Fig. 4; col. 12 lines 56-62)** adapted to generally simultaneously receive protected data from a transmitter **(col. 8 lines 1-10; col. 12 lines 56-62; col. 13 lines 29-33; col. 14 lines 51-59)**, the at least one slave digital terminal being connected to the master terminal by a link **(51, Fig. 4)**,

wherein said slave digital terminal can access said received protected digital data only if information necessary for accessing said protected digital data and received by the master digital terminal is sent by way of said link to the slave digital terminal within a predetermined deadline **(col. 13 lines 11-38; col. 11 line 54- col. 12 line 8; col. 14 line 48- col. 15 line 32; where the predetermined deadline is the validity period or life of the Kex and/or CW. The master device has to send the CW to the slave before its validity changes. Or, when the CW is sent to the slave, it's encrypted**

with a Ks- a session key- that's generated by the slave. This key also has a predetermined time, col. 14 lines 16-24. Without the Ks, no encryption would be possible to transmit CW and no reception of the information necessary for accessing the content would be safely received, which goes against the principle of having a safe link),

wherein the information necessary for accessing said protected digital data **(The CW sent from the master to the slave device, col. 13 lines 11-38; col. 11 line 54- col. 12 line 8; col. 14 line 48- col. 15 line 32, which is encrypted with the session key Ks)** comprises filter parameters **(anything else not encrypted with the Ks, at that point, is filtered or can not be opened)** for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal **(Included with the CW, and also encrypted with the Ks, messages of additional data with additional entitlements for the slave device are sent from the master device, col. 15 lines 4-25).**

On the other hand, Benardeau do not explicitly teach that the digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements.

However, in an analogous art, Akiyama teaches a receiving device that receives access information through a filter that separates incoming packet information based in two selection parameters: content or individual control information used for contract information certification. If the packets include individual control information, it is

extracted in the following steps of the packets' processing ([120]-[0122]; [0125]-[0126]; [0160]; [0224]-[0227]; [0237]; [0248]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified Benardeau's invention with Akiyama's filter for the benefit of having messages included in the content stream, and in this way, avoiding a tentative other channel for the reception of these messages.

6. Claims **23 and 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Benardeau et al. (hereinafter 'Benardeau', Patent No. 6,904,522, which is of record) in view of Peterka et al. (hereinafter 'Peterka', Pub. No. 2002/0170053) in further view of Wehrenberg (Pub. No. 2003/0126445) in view of Akiyama (Pub. No. 2006/0212399) in further view of Noble et al. (hereinafter 'Nobel', Patent No. 7,302,571).

Regarding claims 23 and 24, Bernardeau, Peterka and Wehrenberg teach all the limitations of the claim it depends on. Although Bernardeau teaches having a deadline by which the receiver has to receive the information necessary for accessing encoding data (this predetermined deadline is the validity period or life of the Kex and/or CW, which is in terms of days), Bernardeau do not explicitly teach of another predetermined deadline different from the validity period and equal to a second.

However, in an analogous art, Akiyama teaches a system where out of two communicating devices that are exchanging key information, the one waiting for a response to a challenge from the other device, imposes an additional predetermined

time during which the response needs to arrive. This additional deadline is imposed as another security measure and as a way to authenticate the other device (S408, Fig. 36; S422, Fig. 37; [0173]; [0188]; [0192]; [0197]). Therefore, if an intermediary time delay is added, the response would not arrive on time.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified Bernardeau, Peterka and Wehrenberg's invention with Akiyama's feature of receiving the response from a challenged device in a predetermined period of time for the benefit of having a authenticating the device that is being communicated.

Additionally, Benardeau, Peterka, Wehrenberg and Akiyama teach the limitations as described above. On the other hand, they do not explicitly teach that the second deadline is one second.

However, in an analogous art, Noble teaches a method for making sure that two devices are close to each other within a specified radius, while exchanging keys, by imposing a response time of few times the roundtrip, which is determined to be one second (col. 7 lines 34-67; col. 9 lines 40-50; col. 11 lines 33-44).

Therefore, it would have been obvious to one of ordinary skill in the art to have modified Bernardeau, Peterka, Wehrenberg and Akiyama's invention with Noble's one second response for the benefit of not giving enough time for a physical attack and for ensuring that a device is within a specified range from the other.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OMAR PARRA whose telephone number is (571)270-1449. The examiner can normally be reached on 9-6 PM (M-F, every other Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John W. Miller can be reached on 571-272-7353. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/John W. Miller/
Supervisory Patent Examiner, Art Unit 2421

OP